

**تقدير المخاطر والضبط الداخلي**  
**خواص واعتبارات لأنظمة معلومات تستعمل الحاسوب**  
**RISK ASSESSMENTS AND INTERNAL CONTROL - CIS**  
**CHARACTERISTICS AND CONSIDERATION**

المحتويات	الفقرات
مقدمة	1
الهيكل التنظيمي	2
طبيعة المعالجات	3
التصميم والأوجه الإجرائية	4
الضوابط الداخلية في بيئة نظم المعلومات المحوسبة	5
الضوابط العامة في نظم المعلومات المحوسبة	6-7
الضوابط التطبيقية في نظم المعلومات المحوسبة	8
فحص الضوابط العامة لنظم المعلومات المحوسبة	9
فحص الضوابط التطبيقية لنظم المعلومات المحوسبة	10
التقييم	11

إن هذا البيان الدولي لمهنة التدقيق قد تمت المصادقة عليه من قبل اللجنة الدولية لممارسة مهنة التدقيق في أكتوبر تشرين أول 1991.

يجب على المدقق فهم ومراعاة مميزات بيئة أنظمة المعلومات التي تستعمل الحاسوب بسبب تأثيرها على تصميم النظام المحاسبي والضوابط الداخلية التابعة له، واختيار الضوابط الداخلية التي ينوي المدقق الاعتماد عليها، وفهم طبيعة وتوقيت ومدى الإجراءات.

وقد تم إصدار هذا البيان كملحق للمعيار الدولي للتدقيق (400) المعنون «تقدير المخاطر والضبط الداخلي». وهو لا يشكل جزءاً من المعيار الدولي للتدقيق، ولا يقصد منه أن تكون له صلاحية المعيار الدولي للتدقيق.



## مقدمة

1. إن بيئة نظم المعلومات المحوسبة قد تم تعريفها في المعيار الدولي للتدقيق (401) المعنون «التدقيق في بيئة أنظمة معلومات تستعمل الحاسوب» كما يلي:

لغرض المعايير الدولية للتدقيق فإن بيئة أنظمة المعلومات المحوسبة توجد عندما تستخدم المنشأة الحاسوب، من أي نوع أو حجم، في معالجة المعلومات المالية ذات الأهمية لعملية التدقيق، بغض النظر فيما إذا كان الحاسوب يشغل من قبل المنشأة أو من قبل طرف ثالث.

إن إدخال كافة الضوابط، المرغوب فيها، في نظم المعلومات المحوسبة قد لا يكون عملياً عندما يكون حجم المنشأة صغيراً، أو عند استعمال الحاسوب الشخصي وبغض النظر عن حجم المنشأة. كذلك عندما تعالج البيانات من قبل طرف ثالث، فإن النظرة إلى خواص بيئة نظم المعلومات المحوسبة قد تختلف استناداً لدرجة الوصول إلى معالجات الطرف الثالث. وقد تم وضع سلسلة من البيانات الأولية لمهنة التدقيق كإضافة إلى الفقرات المدرجة أدناه. هذه السلسلة تصف البيانات المختلفة لأنظمة المعلومات المحوسبة، وتأثيرها على النظام المحاسبي ونظام الضبط الداخلي، وعلى إجراءات التدقيق.

## الهيكل التنظيمي

2. في بيئة نظم المعلومات المحوسبة، تقوم المنشأة بتشكيل هيكل تنظيمي وإجراءات لغرض إدارة فعاليات بيئة الأنظمة هذه ويتضمن الهيكل التنظيمي للبيئة الخواص التالية:

- أ- تركيز الوظائف والمعرفة - بالرغم من أن معظم الأنظمة التي تستخدم طرق نظم المعلومات المحوسبة تتضمن بعض العمليات اليدوية، ولكن على العموم، فإن عدد الأشخاص المشاركين في معالجة المعلومات المالية ينخفض بنسبة مهمة. إضافة إلى ذلك، فإن بعض موظفي معالجة البيانات قد يكونوا الوحيدين ممن لديهم معرفة مفصلة عن العلاقات المتبادلة بين مصادر البيانات، وعن كيفية معالجتها وطريقة توزيعها واستعمال مخرجاتها. كذلك من المرجح أن يكونوا مطلعين على أي ضعف في الضبط الداخلي، وعليه فإنهم قد يكونوا في موضع يستطيعون فيه تعديل البرامج أو البيانات خلال تخزينها أو معالجتها، علاوة على ذلك فإن عدة ضوابط تقليدية مستندة إلى فصل ملائم لوظائف متعارضة قد لا تكون موجودة أو في حالة غياب ضوابط الوصول أو الضوابط الأخرى، قد تكون أقل فعالية.
- ب- تركيز البرامج والبيانات - أن المعاملات وبيانات الملف الرئيسي غالباً ما تتركز في صيغة قابلة للقراءة بالآلة، إما في جهاز حاسوب واحد مركزي الموقع، أو في عدة أجهزة موزعة في كافة أرجاء المنشأة، فإن من المرجح أن برامج الحاسوب، التي توفر إمكانية الوصول إلى هذه البيانات وتعديلها، سيتم تخزينها في نفس المواقع التي تكون فيه البيانات. لذا، فإنه في حالة غياب الضوابط المناسبة، فإن هناك احتمالاً بزيادة الوصول غير المرخص إلى هذه البرامج والبيانات وتعديلها.

## طبيعة المعالجات

3. إن استعمال الحاسوب قد ينتج عنه تصميم أنظمة توفر أدلة منظورة، أقل من تلك التي تستعمل الإجراءات اليدوية. بالإضافة إلى ذلك، فإن هذه الأنظمة قد تكون عرضة للوصول من قبل عدد كبير من الأشخاص.

وتتضمن خواص النظام الناتجة من طبيعة معالجات نظم المعلومات المحوسبة ما يلي:

- أ- غياب مستندات المدخلات - قد يتم إدخال البيانات مباشرة إلى نظام الحاسوب بدون مستندات ثبوتية، وفي بعض أنظمة المعاملات المباشرة فإن الأدلة الكتابية بالمصادقة على إدخال بيان منفرد (مثلاً الموافقة على أمر الإدخال) قد يستعاض عنه بإجراءات أخرى، كضوابط التفويض التي تحتوي عليها برامج الحاسوب (مثل الموافقة على حدود الائتمان).
- ب- الافتقار إلى مسار عملية منظورة - قد تكون بعض البيانات محفوظة في ملفات الحاسوب فقط. وفي النظام اليدوي، من الممكن اعتيادياً متابعة المعاملة خلال النظام بواسطة اختبار المستندات الأصلية والدفاتر المحاسبية والسجلات والملفات والتقارير. أما في بيئة نظم المعلومات المحوسبة، فإن جزءاً من مسار العملية قد يكون في صيغة قابلة للقراءة بالآلة، وعلاوة على ذلك فقد تكون موجودة لفترة محدودة من الوقت.
- ج- الافتقار للمخرجات المنظورة - قد لا تكون بعض المعاملات أو نتائج المعالجات مطبوعة. في النظام اليدوي وفي بعض نظم المعلومات المحوسبة، فإنه يمكن عاديّاً اختبار نتائج المعالجات بصرياً، أما في أنظمة المعلومات الأخرى التي تستعمل الحاسوب، فقد لا يتم طبع نتائج المعالجات. لذا فإن فقدان المخرجات المنظورة قد ينتج عنه وجود حاجة للوصول إلى بيانات محفوظة في ملفات قابلة للقراءة بواسطة الحاسوب فقط.
- د- سهولة الوصول إلى البيانات وبرامج الحاسوب - إن البيانات وبرامج الحاسوب قد يتم الوصول إليها وتعديلها بواسطة الحاسوب، أو من خلال استعمال معدات الحاسوب في مواقع بعيدة. وعليه، وفي حالة غياب ضوابط مناسبة، فإن هناك احتمالاً أكبر بإمكانية الوصول غير المرخص إلى البيانات والبرامج وتعديلها، من قبل أشخاص داخل أو خارج المنشأة.

#### التصميم والأوجه الإجرائية.

4. إن تطوير نظم المعلومات المحوسبة، عموماً، تُقضي إلى تصاميم وخواص إجرائية تختلف عن تلك التي نجدها في الأنظمة اليدوية. إن هذه التصاميم والأوجه الإجرائية المختلفة لنظم المعلومات المحوسبة تتضمن ما يلي:
  - أ- ثبات الأداء - تقوم نظم المعلومات المحوسبة بإنجاز الوظائف كما تم برمجتها بالضبط، ومن المحتمل أن تكون أكثر موثوقية من الأنظمة اليدوية، على شرط أن تكون كافة أنواع وشروط المعاملات الممكن حدوثها، قد تم توقعها وأدخلت في النظام. ومن الناحية الأخرى فإن برنامج الحاسوب الذي لم يبرمج ويختبر بشكل صحيح، قد يعالج المعاملات أو البيانات الأخرى بشكل غير صحيح وباستمرار.
  - ب- إجراءات الرقابة المبرمجة - إن طبيعة معالجات الحاسوب تسمح بتصميم إجراءات الضبط الداخلي في برامج الحاسوب. هذه الإجراءات قد تصمم لتوفير ضوابط برؤية محددة (مثلاً، إن حماية البيانات ضد الوصول غير المسموح به قد يتم توفيره بواسطة كلمات السر). أما الإجراءات الأخرى فيمكن تصميمها لاستعمالها بتدخل يدوي، مثل فحص التقارير المطبوعة فيما يتعلق بالاستثناء، وتقارير الأخطاء، وتدقيق المعقولة وحدود البيانات.
  - ج- تحديث ملفات الحاسوب المتعددة أو ملفات قاعدة البيانات بمعاملة منفردة - قد يؤدي إدخال منفرد إلى النظام المحاسبي، إلى تحديث لكافة السجلات المرتبطة مع المعاملة (مثلاً إن إدخال مستندات شحن البضاعة قد تقوم بتحديث ملفات المبيعات وحسابات الزبائن تحت التحصيل، إضافة لتحديث ملف المخزون). لذا فإن أي إدخال غير صحيح في مثل هذا النظام قد يؤدي إلى خلق أخطاء في حسابات مالية متعددة.
  - د- معاملات مولدة من النظام - قد تنشأ بعض المعاملات بواسطة نظام المعلومات التي تستعمل الحاسوب نفسه، وبدون الحاجة إلى مستندات إدخال. إن المصادقة على مثل هذه المعاملات قد لا تظهر بنفس طريقة المعاملات التي تنشأ خارج نظم المعلومات المحوسبة (مثلاً قد يتم احتساب الفائدة وقيداً آلياً على أرصدة حسابات الزبائن استناداً لشروط مصادق عليها مسبقاً تحتوي عليها برنامج الحاسوب).
  - هـ- عدم حصانة وسائط تخزين البيانات والبرامج - قد يتم تخزين الحجم الكبير من البيانات وبرامج

الحاسوب المستعملة لمعالجة هذه البيانات، في وسائط تخزين قابلة للنقل أو ثابتة، كالأقراص والأشرطة المغنطة. هذه الوسائط تكون عرضة للسرقه أو الضياع أو الإهلاك بقصد أو بدون قصد.

### الضوابط الداخلية في بيئة نظم المعلومات المحوسبة

5. إن الضوابط الداخلية على معالجات الحاسوب، والتي تساعد على تحقيق الأهداف العمومية للرقابة الداخلية، تتضمن إجراءات يدوية وإجراءات مصممة في برامج الحاسوب. وتشمل هذه الإجراءات، اليدوية، وبالحاسوب، الضوابط العامة التي تؤثر على بيئة نظم المعلومات المحوسبة (الضوابط العامة) وضوابط خاصة على التطبيقات المحاسبية (الضوابط التطبيقية).

### الضوابط العامة في نظم المعلومات المحوسبة

6. إن غرض الضوابط العامة في نظم المعلومات المحوسبة هو وضع إطار لرقابة كلية على نشاطات هذه الأنظمة، وتوفير مستوى ثقة معقولة بأن الأهداف الكلية للرقابة الداخلية قد تحققت. وتتضمن الضوابط العامة في نظم المعلومات المحوسبة ما يلي:

- أ- ضوابط التنظيم والإدارة - مصممة لوضع إطار تنظيمي على نشاطات أنظمة المعلومات التي تستعمل الحاسوب، وتتضمن:
  - سياسات وإجراءات تتعلق بوظائف الرقابة.
  - فصلاً ملائماً للوظائف المتعارضة (مثل إعداد معاملات الإدخال والبرمجة، تشغيل الحاسوب).
- ب- ضوابط تطوير وصيانة الأنظمة التطبيقية - مصممة لتوفير ثقة معقولة بأن الأنظمة يتم تطويرها والحفاظ عليها بطريقة مرخصة وكفوءة. وهي أيضاً مصممة نموذجياً لوضع ضوابط على:
  - اختبار وتحويل وتطبيق وتوثيق الأنظمة الجديدة أو المعدلة.
  - تغييرات على الأنظمة التطبيقية.
  - الوصول إلى الأنظمة الموثقة.
  - اكتساب أنظمة تطبيقية من أطراف ثالثة.
- ج- ضوابط تشغيل الحاسوب - مصممة للرقابة على تشغيل الأنظمة، وتوفير ثقة معقولة بأن:
  - الأنظمة قد تم استعمالها لأغراض مرخصة فقط.
  - الوصول إلى عمليات الحاسوب مقيد بالأشخاص المخولين.
  - البرامج المرخصة هي المستعملة فقط.
  - أخطاء المعالجات قد تم اكتشافها وتصحيحها.
- د. ضوابط برمجيات الأنظمة - مصممة لتوفير ثقة معقولة بأن برمجيات النظام قد تم اكتسابها أو تطويرها بطريقة مرخصة وكفوءة، وتتضمن:
  - المصادقة والموافقة والاختبار والتطبيق والتوثيق لبرمجيات الأنظمة الجديدة، وللتعديلات على برمجيات الأنظمة الحالية.
  - تقييد الوصول إلى برمجيات الأنظمة والتوثيق للموظفين المخولين فقط.
- هـ. ضوابط إدخال البيانات والبرامج - مصممة لتوفير ثقة معقولة بأن:
  - قد تم وضع هيكلية للمصادقة على المعاملات التي يتم إدخالها في النظام.
  - وإن الوصول إلى البيانات والبرامج مقيد بالموظفين المخولين.

7. هنالك إجراءات وقائية أخرى لنظم المعلومات المحوسبة والتي تسهم باستمرار المعالجات في هذه الأنظمة. وقد تتضمن:

- إسناداً من خارج الموقع للبيانات والبرامج.
- إجراءات الاستعادة لاستعمالها في حالة السرقة أو الفقدان أو الإهلاك المقصود أو غير المقصود.

- توفير معالجات خارج الموقع في حالة حدوث كارثة.
  - الضوابط التطبيقية في نظم المعلومات الحوسبة
8. إن الغرض من الضوابط التطبيقية لنظم المعلومات الحوسبة هو وضع إجراءات رقابة محددة على التطبيقات الحاسوبية، لأجل توفير ثقة معقولة بأن كافة المعاملات قد تمت المصادقة عليها وتسجيلها، كما تمت معالجتها بالشكل الكامل والدقيق وفي الوقت المناسب. وتتضمن الضوابط التطبيقية في أنظمة المعلومات التي تستعمل الحاسوب ما يلي:

- أ- الضوابط على المدخلات - مصممة لتوفير ثقة معقولة بأن:
    - المعاملات قد تمت المصادقة عليها بشكل مناسب، قبل معالجتها بواسطة الحاسوب.
    - المعاملات قد تمت تحويلها بدقة إلى صيغة قابلة للقراءة بالآلة، وتم تسجيلها في ملفات بيانات الحاسوب.
    - عدم ضياع المعاملات أو إضافتها أو تكرارها أو تغييرها بشكل غير مناسب.
    - المعاملات غير الصحيحة قد تم رفضها وتصحيحها، وفي حالة الضرورة، إعادة إدخالها في الوقت المناسب.
  - ب- ضوابط على المعالجات وملفات بيانات الحاسوب - مصممة لتوفير ثقة معقولة بأن:
    - المعاملات، بما فيها المعاملات المولدة من النظام، قد تمت معالجتها بواسطة الحاسوب بالشكل المناسب.
    - عدم ضياع المعاملات أو إضافتها أو تكرارها أو تغييرها بشكل غير مناسب.
    - أخطاء المعالجات قد تم تحديدها وتصحيحها في الوقت المناسب.
- الضوابط على المخرجات - مصممة لتوفير ثقة معقولة بأن:
- نتائج المعالجات كانت دقيقة.
  - الوصول إلى المخرجات مقيد بالموظفين المخولين فقط.
  - المخرجات قد تم تقديمها إلى الموظفين المخولين الملائمين في الوقت المناسب.

### فحص الضوابط العامة لنظم المعلومات الحوسبة

9. لقد تم وصف الضوابط العامة في نظم المعلومات الحوسبة، والتي قد يرغب المدقق في اختبارها، في الفقرة (6). وعلى المدقق دراسة كيفية تأثير هذه الضوابط العامة على تطبيقات نظم المعلومات الحوسبة، والتي لها أهمية على عملية التدقيق. ونموذجياً، فإن الضوابط العامة في نظم المعلومات الحوسبة والمتعلقة ببعض أو كافة التطبيقات، هي ضوابط يعتمد بعضها على بعض، وذلك لأن عملها غالباً ما يكون ضرورياً لفعالية الضوابط التطبيقية لنظم المعلومات الحوسبة. لذا، فقد يكون أكثر فعالية أن يتم فحص تصميم الضوابط العامة قبل فحص الضوابط التطبيقية.

### فحص الضوابط التطبيقية لنظم المعلومات الحوسبة

10. يتم تنفيذ الضوابط على المدخلات والمعالجات وملفات البيانات والمخرجات من قبل موظفي المعلومات التي تستعمل الحاسوب، أو مستخدم النظام، أو مجموعة سيطرة منفصلة، أو قد تبرمج في البرمجيات التطبيقية. وتتضمن الضوابط التطبيقية أنظم المعلومات الحوسبة، والتي قد يرغب المدقق باختبارها ما يلي:

- أ. ضوابط يدوية تمارس من قبل المستخدمين - في حالة كون الضوابط اليدوية التي تمارس من قبل مستخدم النظام التطبيقي، قابلة لتوفير ثقة معقولة بأن مخرجات النظام كاملة ودقيقة ومصادق عليها، فقد يقرر المدقق تحديد اختبارات الرقابة بالضوابط اليدوية هذه (مثلاً قد تتضمن الضوابط اليدوية التي تمارس من قبل المستخدمين على نظام الرواتب الآلي، مجموعاً رقابياً توقعياً للمدخلات بإجمالي الأجور، وتدقيق اختباري لاحتسابات مخرجات صافي الرواتب، وموافقات الدفع وتحويل الأموال، والمقارنة مع مبالغ سجل الرواتب، ومطابقة حساب المصرف الفوري). في مثل هذه الحالة، قد يرغب المدقق بالاكتماء باختبار الضوابط اليدوية التي تمارس من قبل المستخدمين.

ب. معلومات منتجة من قبل الحاسوب أو تحتويها برامج الحاسوب، وذلك إضافة للضوابط اليدوية التي تمارس من قبل المستخدمين، فقد يمكن اختبار هذه الضوابط باختبار مخرجات النظام، إما باستعمال طرق يدوية أو طرق التدقيق بمساعدة الحاسوب. هذه المخرجات قد تكون على شكل وسائط ممغنطة أو شريط مصغر (ميكروفيلم) أو مطبوعات (مثلاً، قد يختبر المدقق الضوابط التي تمارس من قبل المنشأة على مطابقات مجاميع التقارير مع الحسابات الرقابية في الأستاذ العام، وقد ينجز اختبارات يدوية على هذه المطابقات). وكبديل عند إجراء المطابقة بالحاسوب، فقد يرغب المدقق باختبار المطابقة وذلك عن طريق إعادة إجراء الرقابة باستعمال طرق التدقيق بمساعدة الحاسوب (لاحظ البيان الدولي لمهنة التدقيق (1009) المعنون «طرق التدقيق بمساعدة الحاسوب»).

ج. إجراءات الرقابة المبرمجة - في حالة بعض أنظمة الحاسوب، قد يجد المدقق بأنه من غير الممكن، أو في بعض الحالات من غير العملي، اختبار الضوابط عن طريق اختبار ضوابط المستخدمين أو مخرجات النظام فقط (مثلاً في التطبيقات التي لا توفر مطبوعات لموافقات هامة أو تجاهل للسياسات العادية، قد يرغب المدقق في اختبار إجراءات الرقابة الموجودة داخل البرنامج التطبيقي). حيث قد يقوم المدقق بدراسة إنجاز اختبارات الرقابة، وذلك باستعمال طرق التدقيق بمساعدة الحاسوب، كاختبار البيانات، أو إعادة معالجة البيانات العملية، أو في الحالات غير الاعتيادية، اختبار ترميز البرنامج التطبيقي.

### التقييم

11. قد يكون للضوابط العامة في نظم المعلومات المحوسبة تأثيراً شاملاً على معالجة البيانات في الأنظمة التطبيقية. وفي حالة كون هذه الضوابط غير فعالة، فقد تكون هناك مخاطر بأن معلومات خاطئة قد تحدث وتمر بدون اكتشاف في البرامج التطبيقية. لذا فإن أي ضعف في الضوابط العامة لنظم المعلومات المحوسبة قد يمنع من اختبار بعض الضوابط التطبيقية في أنظمة المعلومات التي تستعمل الحاسوب، ومع ذلك، فإن الإجراءات اليدوية التي يمارسها المستعملون قد توفر رقابة فعالة على المستوى التطبيقي.

